EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Randy Noranbrock (Reg. No. 42,940) on August 13, 2008.

The application has been amended as follows:

1. Claim 20 is cancelled by virtue of this Examiner's Amendment.
2. Claims 14-19 are amended by virtue of this Examiner's Amendment.

Claim 14 (Currently Amended):

A system for detecting critical file changes, comprising:

a processor; and

a memory storing instructions which, when executed by the processor, cause the processor to:

generate a read request for an event from an intrusion detection data source (IDDS), wherein the event is a kernel audit record removed from a buffer;

reading the requested event;

route events to a template, wherein the event comprises one or more parameters and the template comprises a sequence of connected logic nodes comprising at least one input node, at least one filter node, and at least one output node,

filter the event, based on the template, as a possible intrusion based on one of the one or more parameters and either dropping the event or outputting the event, wherein the instructions causing the processor to determine a filename based on the event and output the event for each event indicating modification of a critical file based upon the determined filename, and

create an intrusion alert for each event output from the filter.

Claim 15 (Currently Amended):

The system of claim ~~20~~14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the permission bits on a file or directory.

Claim 16 (Current Amended):

The system of claim ~~20~~14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating that a file was opened for truncation.

Claim 17 (Currently Amended):

The system of claim ~~20~~14, wherein the instructions causing the processor to filter the event comprise instructions causing the processor to provide the event to the determine a filename instructions for each event comprising one of the one or more parameters indicating modification of the ownership or group ownership of a file.

Claim 18 (Currently Amended):

The system of claim ~~20~~14, wherein the instructions further comprise instructions causing the processor to output an alert message for each renamed file, the alert message comprising the filename of the file and the filename of the renamed file.

Claim 19 (Currently Amended):

The system of claim ~~20~~14, wherein the instructions causing the processor to configure a template based on a list of files and directories to be included or excluded based on whether the files and directories are considered unmodifiable.

REASONS FOR ALLOWANCE

1. Claims 1-6, 13-19, and 21-24 are allowed.

2. The following is an examiner's statement of reasons for allowance:

3. No prior art teaches or renders obvious all of the limitations in independent claims 1 and 14, and the subsequent dependent claims.

4. Specifically, the claimed invention generally concerns a method and system for detecting critical file changes by generating a read request for an event representing a system call, wherein the event is a kernel audit record removed from a buffer of an intrusion detection source, reading the event, routing the event to a template, and filtering the event, wherein the filtering comprises determining a filename based on the event, and outputting the event indicating the modification of a critical file based upon the determined filename, and outputting an alert based on the filtering. The prior art does not teach the above invention.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/

Examiner, Art Unit 2131

/K. A./

08/14/2008

Examiner, Art Unit 2431